AMENDMENTS TO THE CLAIMS

1-45.   (Cancelled)

46.   (Currently amended) A data processor for receiving and processing data to which information for tampering detection is added, said data processor comprising:

a receiver operable to receive data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection, wherein the protected data region includes an unprotection list which lists, ~~by type,~~ tag names indicating types of the data included in the unprotected data region;

a protected data authentication unit operable to detect, for the data, which is included in the protected data region and received by said receiver, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region; and

an unprotected data authentication unit operable to determine the data included in the unprotected data region as being valid when a ~~data~~ tag name indicating a type of the data, which is included in the unprotected data region and received by said receiver, coincides with a ~~data type~~ tag name in the unprotection list which has been confirmed as not having been tampered with by said protected data authentication unit.

47.   (Previously Presented) The data processor according to claim 46, wherein:

the data received by said receiver is hypertext data; and

the unprotection list lists, by type, a tag included in the unprotected data region.

48.   (Currently amended) A data processor structured by a transmitting data processor and a receiving data processor, said transmitting data processor being operable to transfer, to said receiving data processor, data to which information for tampering detection is added,

wherein said transmitting data processor comprises:

an unprotection list generation unit operable to generate an unprotection list which lists, by type, data that is not to be subjected to tampering detection;

a data generation unit operable to generate data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region; and

a transmitter operable to transmit the data generated by said data generation unit; and

wherein said receiving data processor comprises:

a receiver operable to receive the data transmitted from said transmitting data processor;

a protected data authentication unit operable to detect, for the data, which is included in the protected data region and received by said receiver, whether the data in the protected data region has been tampered by using the tampering detection information in the authentication information region; and

an unprotected data authentication unit operable to determine the data included in the unprotected data region as being valid when a ~~data~~ tag name indicating a type of the data, which is included in the unprotected data region and received by said receiver, coincides with a ~~data type~~ tag name in the unprotection list which has been confirmed as not having been tampered with by said protected data authentication unit.

49.   (Previously Presented) The data processor according to claim 48, wherein:

the data generated by said data generation unit is hypertext data; and

the unprotection list lists, by type, a tag included in the unprotected data region.

50.   (Currently amended) A data processing method for receiving and processing data to which information for tampering detection is added, said method comprising:

receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection, the protected data region including an unprotection list which lists~~, by type,~~ <u>tag names indicating types of</u> the data included in the unprotected data region;

detecting, for the data, which is included in the protected data region and received in said receiving of the data, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region; and

determining the data included in the unprotected data region as being valid when a ~~data~~<u>tag name indicating a</u> type of the data, which is included in the unprotected data region and received in said receiving of the data, coincides with a ~~data type~~<u>tag name</u> in the unprotection list which has been confirmed as not having been tampered with in said detecting whether the data included in the protected data region has been tampered with.

51.　　(Currently amended) A data processing method for transferring data, to which information for tampering detection is added, from a transmitting data processor to a receiving data processor, wherein:

in the transmitting data processor, said method comprises

generating an unprotection list which lists, by type, data that is not to be subjected to tampering detection,

generating data to be transmitted by arranging data to be subjected to tampering detection together with the unprotection list in a protected data region, the data that is not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in the protected data region in an authentication information region, and

transmitting the data generated in said generating of the data to be transmitted; and

in the receiving data processor, said method comprises

receiving the data transmitted from the transmitting data processor,

detecting, for the data, which is included in the protected data region and received in said receiving of the data, whether the data in the protected data region has been tampered with by using the tampering detection information in the authentication information region, and

determining the data included in the unprotected data region as being valid when a ~~data~~tag name indicating a type of the data, which is included in the unprotected data region and received in said receiving of the data, coincides with a ~~data type~~tag name in the unprotection list which has been confirmed as not having been tampered with in said detecting whether the data in the protected data region has been tampered with.

52-58. (Cancelled)